Opening Statement of the Honorable Greg Walden
Subcommittee on Communications and Technology
Hearing on "Cybersecurity: An Examination of the Communications Supply Chain"
May 21, 2013

(As Prepared for Delivery)

Our communications network's strengths — its ubiquity and interconnected nature — may also be weaknesses. Those who wish to harm our nation, to steal money or intellectual property, or merely to cause mischief, can focus on myriad hardware and software components that make up the communications infrastructure. And they can do so anywhere in the design, delivery, installation or operation of those components. Today's hearing will focus on securing that communications supply chain.

We are fortunate to have as a member of this subcommittee House Intelligence Committee Chairman Mike Rogers. The experience and resources he brings were invaluable to the bipartisan cybersecurity working group last Congress as well as this subcommittee's three prior cyber hearings. Many of us have concluded that promoting information sharing through the Cyber Intelligence Sharing and Protection Act that he and Rep. Ruppersberger have now twice ushered through the House is pivotal to better securing our networks. It was also in large part his committee's 2012 report on the communications supply chain that prompted this hearing. Supply chain risk management is essential if we are to guard against those that would compromise network equipment or exploit the software that runs over and through it.

Understanding that you can never eliminate these risks, how do you minimize them without compromising the interconnectivity that makes networks useful? How secure is the communications supply chain? Where are the vulnerabilities? How much should we focus on securing physical access to components as they make their way from design to installation? How much on the internal workings of the components themselves? How do the risks and responses differ for hardware and software? What about for internationally sourced products as opposed to domestic ones? What progress has been made through public-private partnerships, standards organizations and the development of best practices? What role should the government play?

These are among the questions we will examine in this hearing, as well as through the bipartisan supply chain working group we launch today. Reps. Mike Rogers and Anna Eshoo will co-chair the group, which will also include Reps. Latta, Doyle, Terry, Lujan, Kinzinger, and Matheson. As I did last Congress, I will urge that we abide by a cyber Hippocratic Oath and first do no harm as we consider the tools available to the public and private sectors in making our communications supply chain secure.

###